PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/00 — A1

(11) International Publication Number: WO 98/15082

(43) International Publication Date: 9 April 1998 (09.04.98)

(21) International Application Number: PCT/US97/13520

(22) International Filing Date: 30 July 1997 (30.07.97)

(30) Priority Data:
08/724,176 30 September 1996 (30.09.96) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor: DAVIS, Derek, L.; 4509 E. Desert Trumpet Road, Phoenix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

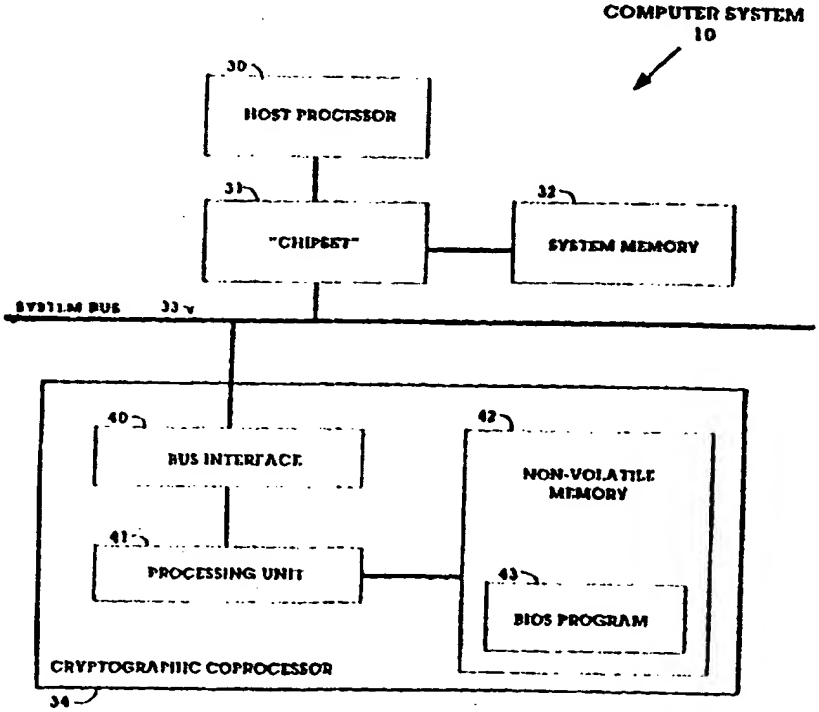
(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: SECURE BIOS

(57) Abstract

A subsystem prevents unauthorized modifications of BIOS program code embedded in modifiable non–volatile memory devices such as flash memory. A cryptographic coprocessor (34) containing the BIOS memory device (42) performs authentication and validation on the BIOS upgrade based on a public/private key protocol. The authentication is performed by verifying the digital signature embedded in the BIOS upgrade.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SECURE BIOS

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to the field of security of computer firmware, especially in the areas of Basic Input and Output System ("BIOS") in general computing systems, such as personal computers ("PCs").

2. Description of Related Art

One of the most critical elements in a computer system is the boot-up firmware, such as the Basic Input and Output System ("BIOS"). Typically stored in some form of non-volatile memory, the BIOS is machine code, usually part of an Operating System ("OS"), which allows the Central Processing Unit ("CPU") to perform tasks such as initialization, diagnostics, loading the operating system kernel from mass storage, and routine input/output ("I/O") functions.

Upon power up, the CPU will "boot up" by fetching the instruction code residing in the BIOS. Due to its inherent nature, the BIOS has two conflicting requirements: (1) it should be well protected because if it is modified or destroyed, the entire system will fail, (2) it should be easily modifiable to allow field upgrade for feature enhancement or removal of software bugs.

Traditionally, BIOS is implemented in Erasable Programmable Read Only Memory ("EPROM"). EPROM has an advantage of not being modified in circuit. To modify the contents of the EPROM, the device must be first erased by being removed from the socket and exposed to Ultraviolet light for a prolonged period of time. In this respect, BIOS implemented in EPROM is resistant to virus attack and other electronic

sabotages. However, EPROM devices do not support "field upgrades" because these devices are not in-circuit programmable, which is a necessary characteristic for field upgrades. Field upgrading allows customers to upgrade the BIOS in the field to avoid costly delay and parts exchanges. Because of the importance for field upgrading, virtually all BIOS firmware is now implemented using flash memories. However, being field modifiable, BIOS flash memories are vulnerable to virus attacks which could cause devastating results in sensitive applications such as financial transactions.

With no security protection, conventional computer architectures implemented with BIOS flash memories are vulnerable to many kinds of intrusive attacks, such as a virus attack. In a typical virus attack, the virus code executes a code sequence to modify the BIOS flash memory. The code in BIOS flash memory, having no protection, is corrupted and the destructive effects may become effective immediately, when the system is booted up the next time, or when certain conditions or events have occurred. The infected code may further propagate to other areas of the BIOS code or the operating system kernel. Because the BIOS is the first program code to execute when the computer system is "powered up", prior to any system or network virus scanning software, detection and eradication of a BIOS-based virus is extremely difficult. The BIOS-based virus can "hide its tracks" from such scanning software, effectively becoming invisible.

The primary focus of the present invention, therefore, is to prevent corrupting the BIOS by a computer virus. This is achieved by imposing an authentication and validation procedure before the contents of the BIOS flash memory are modified.

The approach which is pursued in this invention builds on the concept of BIOS authentication by incorporating the BIOS flash memories into existing hardware with authenticating capability such as the cryptographic coprocessor. Since the cryptographic coprocessor both stores the BIOS and enforces authentication of BIOS updates, an attacker has no means by which to corrupt the BIOS contents.

SUMMARY OF THE INVENTION

The present invention describes a system to securely update an executable code. The system comprises of a first storage element for storing a code update, a second storage element for storing the executable code that needs to be updated, an identification code for identifying the first storage element and the code update, and a security processor. The security processor is coupled to the second storage element to authenticate and validate the first storage element and the code update using the device identification.

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become apparent from the following detailed description of the present invention in which:

Figure 1 is a diagram of the present invention where the BIOS flash memory resides inside a cryptographic coprocessor which may be interfaced to the PCI bus.

Figure 2 is a flowchart of the operations that occur in the present invention during a normal read access to the BIOS program by the host processor.

Figure 3 is a flowchart of the operations that occur in the present invention during a field upgrade of the BIOS program.

DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a procedure to authenticate and validate a code update, such as a BIOS upgrade for example, using cryptographic technology. In the following description, some terminology is used to discuss certain cryptographic features. A "key" is an encoding and/or decoding parameter used by conventional cryptographic algorithms such as Rivest, Shamir and Adleman ("RSA"), Data Encryption Algorithm ("DEA") as specified in Data Encryption Standard ("DES") and the like. A "certificate" is defined as any digital information (typically a public key) associated with an entity, encrypted by a private key held by another entity such as a manufacturer or a widely published trusted authority (e.g., bank, governmental entity,

trade association, etc.). A "digital signature" is similar to a certificate but is typically used for authenticating data. Herein, the term "secure" indicates that it is computationally infeasible for an interloper to successfully perpetuate fraud on a system. A security processor is an electronic device capable of performing security functions to provide security protection for the system.

The authentication and validation are performed by a security processor which contains the BIOS firmware. One example of such a security processor is a cryptographic coprocessor. The cryptographic processor authenticates and validates the BIOS firmware by using secret information such as a digital signature embedded in the BIOS upgrade.

Referring to **Figure 1**, an embodiment of a computer system implemented within the present invention is shown. The computer system 10 includes a chipset 31 which operates as an interface to support communications between host processor 30, system memory 32, and devices coupled to a system bus 33. System memory 32 may include, but is not limited to conventional memory such as various types of random access memory ("RAM"), e.g., DRAM, VRAM, SRAM, etc., as well as memory-mapped I/O devices. System bus 33 may be implemented in compliance with any type of bus architecture including Peripheral Component Interconnect ("PCI"), a Universal Serial Bus ("USB") and the like.

One of the devices that may be coupled to the system bus 33 includes a cryptographic coprocessor 34. Cryptographic coprocessor 34 comprises a bus interface 40, a processing unit 41 and a local non-volatile memory 42. The bus interface 40 is used to establish an electrical connection to system bus 33. Processing unit 41 is used as the main controller for the cryptographic coprocessor 34. Processing unit 41 interfaces to its own local non-volatile memory 42. The boot-up program 43 is stored within non-volatile memory 42. It is contemplated that non-essential elements have not been illustrated to avoid obscuring the present invention. Examples of the non-essential elements that may be employed within the cryptographic coprocessor 34 include RAM, a random number generator, and various cryptographic algorithm accelerators. Furthermore, although host processor 30 is shown separate from

cryptographic coprocessor 34 in **Figure 1**, cryptographic coprocessor 34 may be part of host processor 30 in which case host processor 30 accesses the BIOS program directly without going through system bus 33.

In **Figure 2,** the steps associated with the "boot up" phase of the system are shown. First, in step 50, the host processor issues a read request for an address corresponding to the BIOS program. The cryptographic coprocessor responds to that request with the associated BIOS instruction (Step 60). Lastly, the host processor processes that data in step 70. To continue processing BIOS instructions, this sequence is repeated.

In a typical field BIOS upgrade, the software manufacturer (the BIOS vendor) will send the user a diskette containing the new BIOS code, and the code to perform the upgrade operations. It is also possible for the BIOS vendor to establish a bulletin board system, or a data superhighway connection such as the Internet, to allow users to download the BIOS upgrade electronically and remotely. BIOS upgrading essentially involves erasing and writing to the BIOS flash memory.

In **Figure 3**, the steps associated with a modification of the BIOS program are shown. In step 110, the host processor issues a "replace BIOS" command to the cryptographic coprocessor. This command would typically be generated by some type of BIOS management utility software, running either on the host processor itself or on a remote system. The purpose of this command is to prepare the cryptographic coprocessor for a new BIOS program (step 120). In step 130, the cryptographic coprocessor either passively receives the new BIOS program code from the host processor or actively retrieves it from a specified source (e.g. system memory). In step 140, the new BIOS program is stored internally or in a protected manner to assure that future authentication operations are performed on the specified "new BIOS program". In step 150, the cryptographic coprocessor performs the appropriate authentication operations on this internally stored version of the new BIOS program. There are many ways such authentication can be performed, including the use of secret information known only to the BIOS provider and the deployed cryptographic coprocessor. It is contemplated that public/private key cryptography may be used as

part of the authentication procedure, specifically using the well-known techniques of digital signatures and certificates to validate the integrity and validity of the "new BIOS program". Whatever authentication technique is used, the salient feature is that it is performed within the cryptographic coprocessor on the local version of the new BIOS program. Once the authentication operations have been performed, in step 160, the cryptographic coprocessor can make a determination as to the validity of the new BIOS program. For example, the digital signature supplied with the "new BIOS program" may be valid, but the revision date may be inappropriate (e.g. older than the currently installed BIOS). If the new BIOS is determined to be invalid, it is deleted by the cryptographic coprocessor and is never used (step 170). If the new BIOS is valid, the new BIOS program is made operational and the previous BIOS program is deleted (step 180). Note that at this point, it would be normal to reboot the computer system to assure system-wide consistency.

To support this digital signature-based method of BIOS authentication, the digital signature embedded in the distribution BIOS software upgrade should be underwritten or endorsed by an industry association, or a similar organization or procedure. The participants in this industry association are the BIOS vendors who want to be able to field upgrade their BIOS code. One of the functions of this industry association is to issue digital certificates to its BIOS vendor members, essentially assigning a digital certificate to each vendor to be used in BIOS upgrade software. This association provides its public key to be used by the cryptographic coprocessor during the BIOS authentication procedure. The cryptographic coprocessor will be preloaded with the public key of the industry association for BIOS vendors so that it will be able to verify any digital signature embedded in the BIOS upgrade code. Alternatively, the cryptographic coprocessor may be preloaded with another public key that may be used to authenticate a certificate chain to obtain this industry association public key. The BIOS upgrade code could be encrypted if necessary (to protect the code from being reverse engineered for example). Since the digital signature or the certificate issued by the industry association normally represents the authenticity of a reputable or credible BIOS vendor, an intruder cannot corrupt the BIOS code (unless of course he or she

somehow obtains secret private keys used to create such signatures or certificates) either directly or indirectly by virus attack.

In another embodiment (not shown), the cryptographic coprocessor is part of the host processor. The host processor contains both the cryptographic coprocessor and the BIOS program. The host processor, acting itself as the security processor, performs the authentication and validation on the BIOS upgrade in the similar fashion as described above. The host processor will be preloaded with the public key of the industry association for BIOS vendors so that it will be able to verify any digital signature embedded in the BIOS upgrade code.

Yet, in another embodiment (not shown), the BIOS program is located in a printed-circuit board ("PCB") or card plugged into a system expansion slot. The cryptographic coprocessor may be located on the same PCB or card or on another PCB or card or even inside the host processor. Regardless whether it is located in the system, as long as the cryptographic coprocessor is able to access the BIOS program, it can carry out the authentication and validation operations as described above.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to which the invention pertains are deemed to lie within the spirit and scope of the invention.

CLAIMS

What is claimed is:

1. A system for securely updating an executable code, comprising:
first storage means for storing a code update;
second storage means for storing said executable code; and
first processing means for authenticating and validating said first storage means and said code update based on a device identification, said first processing means being coupled to said second storage means.

2. The system of claim 1 wherein the executable code is a Basic Input and Output System.

3. The system of claim 1 wherein the first storage means is one of a mass storage device and a file capable of being sent electronically in a computer network.

4. The system of claim 1 wherein the second storage means is a modifiable non-volatile memory device.

5. The system of claim 1 wherein the first processing means includes a cryptographic processor.

6. The system of claim 1 wherein the device identification received by the first processing means includes a digital signature.

7. The system of claim 1 wherein said executable code is encrypted to produce an encrypted code.

8. The system of claim 1 further comprising:

second processing means for communicating with said first processing means in order to execute said executable code.

9. The system of claim 7 wherein said encrypted code is decrypted to produce a decrypted code.

10. A system for securely updating an executable code, comprising:
a first storage element that contains a code update;
a second storage element that contains said executable code; and
a security processor coupled to said second storage element, said security processor authenticating and validating said first storage element and said code update based on a device identification.

11. The system of claim 10 wherein the executable code is a Basic Input and Output System.

12. The system of claim 10 wherein the first storage element is one of a mass storage device and a file capable of being sent electronically in a computer network.

13. The system of claim 10 wherein the second storage element is a modifiable non-volatile memory device.

14. The system of claim 10 wherein the security processor is a cryptographic processor.

15. The system of claim 10 wherein said device identification received by said security processor includes a digital signature.

16. The system of claim 10 wherein said executable code is encrypted to produce an encrypted code.

17. The system of claim 10 further comprising:
a host processor for communicating with said security processor in order to execute said executable code.

18. The system of claim 16 wherein said encrypted code is decrypted to produce a decrypted code.

19. A method for securely updating an executable code, the method comprising the steps of:
providing a first storage element for storing a code update;
providing a second storage element for storing said executable code;
configuring said first storage element to contain a device identification;
providing a security processor for accessing said second storage element;
authenticating said first storage element based on said device identification by said security processor; and
updating said executable code by said code update if said first storage element is authenticated.

20. The method of claim 19, wherein before said updating step, the method further comprises a step of validating said code update in the first storage element.

21. The method of claim 19 wherein the executable code is a Basic Input and Output System.

22. The method of claim 19, wherein said executable code provided in the second storage element is in an encrypted format.

23. The method of claim 19 further comprising:
providing a host processor for communicating with said security processor in order to execute said executable code.

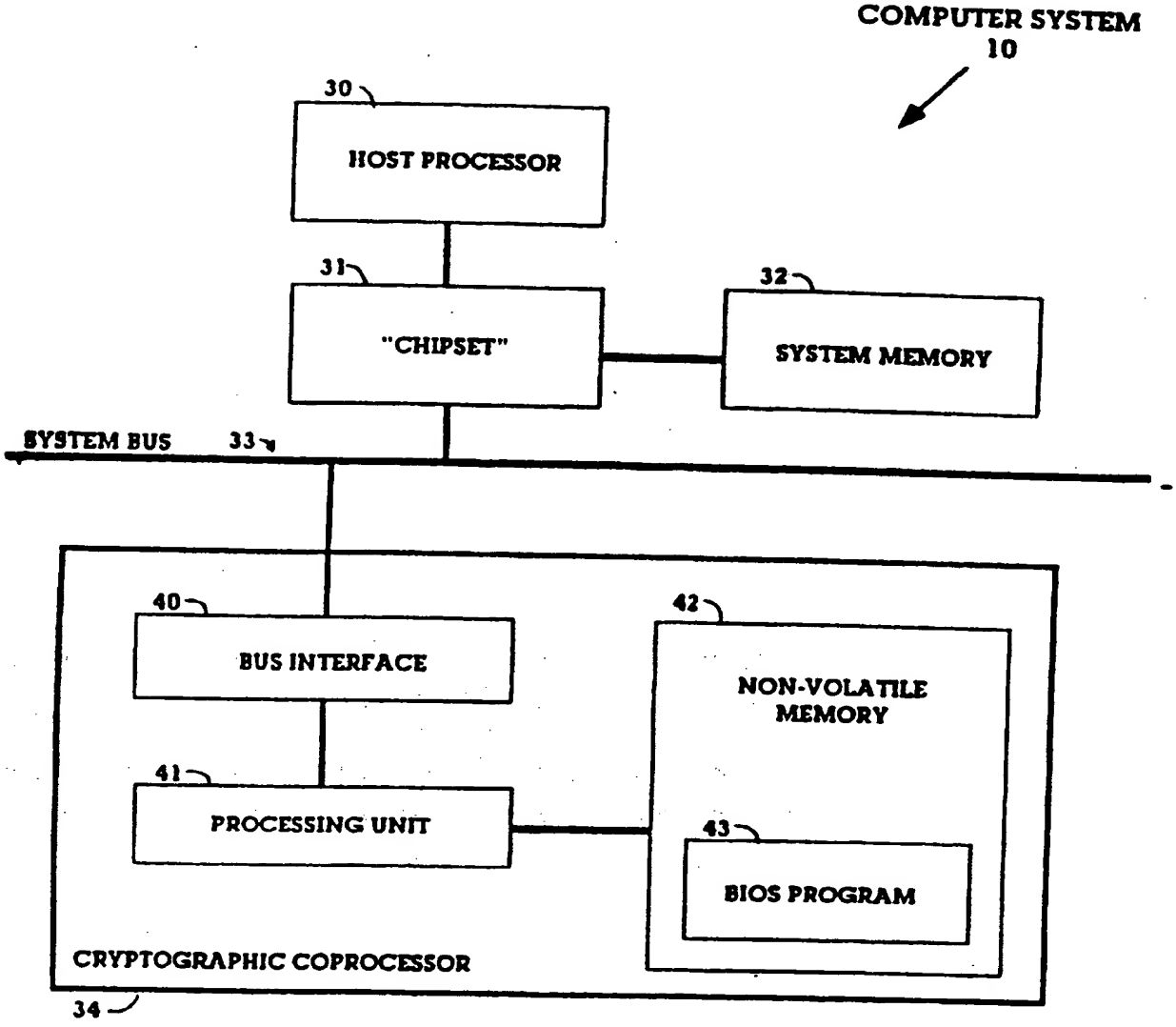

COMPUTER SYSTEM
10
30
HOST PROCESSOR
31
"CHIPSET"
32
SYSTEM MEMORY
SYSTEM BUS
33
40
BUS INTERFACE
41
PROCESSING UNIT
42
NON-VOLATILE MEMORY
43
BIOS PROGRAM
CRYPTOGRAPHIC COPROCESSOR
34

FIGURE 1

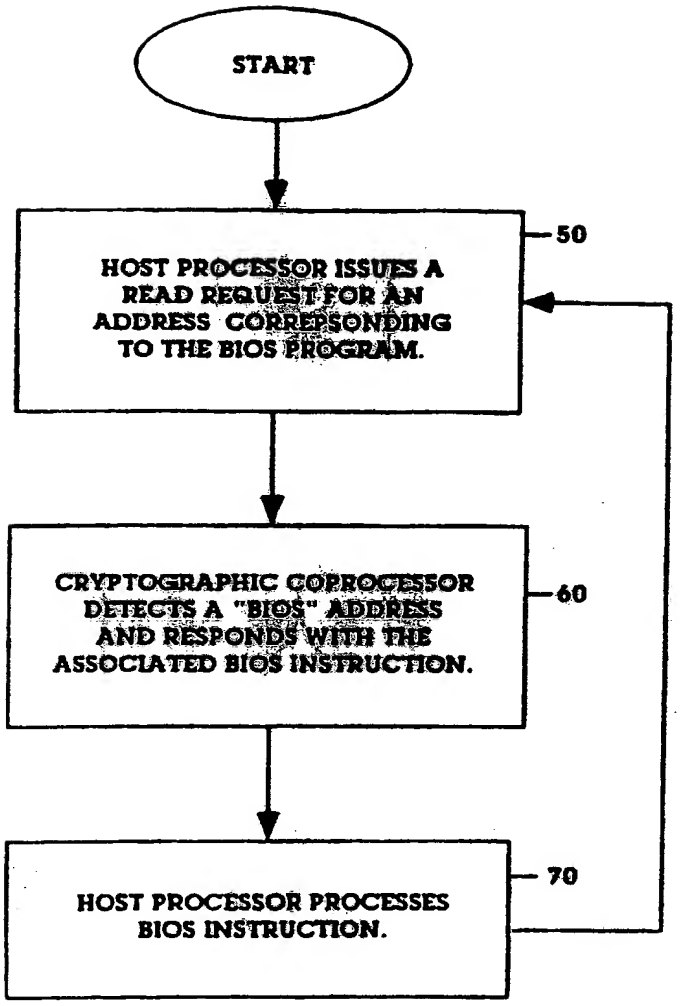

START
HOST PROCESSOR ISSUES A READ REQUEST FOR AN ADDRESS CORRESPONDING TO THE BIOS PROGRAM.
50
CRYPTOGRAPHIC COPROCESSOR DETECTS A "BIOS" ADDRESS AND RESPONDS WITH THE ASSOCIATED BIOS INSTRUCTION.
60
HOST PROCESSOR PROCESSES BIOS INSTRUCTION.
70

FIGURE 2

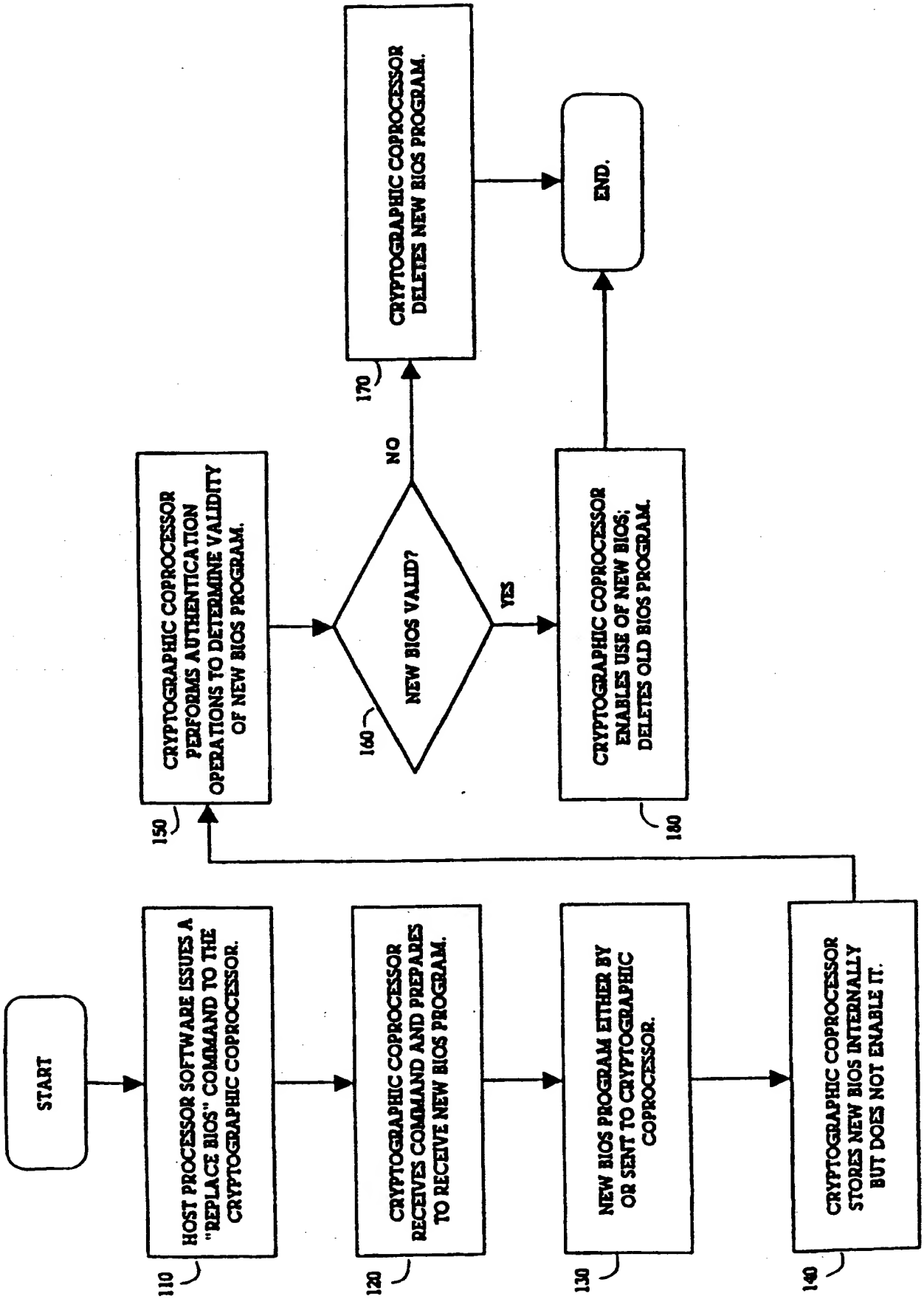

START
HOST PROCESSOR SOFTWARE ISSUES A "REPLACE BIOS" COMMAND TO THE CRYPTOGRAPHIC COPROCESSOR.
110
CRYPTOGRAPHIC COPROCESSOR RECEIVES COMMAND AND PREPARES TO RECEIVE NEW BIOS PROGRAM.
120
NEW BIOS PROGRAM EITHER BY OR SENT TO CRYPTOGRAPHIC COPROCESSOR.
130
CRYPTOGRAPHIC COPROCESSOR STORES NEW BIOS INTERNALLY BUT DOES NOT ENABLE IT.
140
CRYPTOGRAPHIC COPROCESSOR PERFORMS AUTHENTICATION OPERATIONS TO DETERMINE VALIDITY OF NEW BIOS PROGRAM.
150
NEW BIOS VALID?
160
NO
YES
CRYPTOGRAPHIC COPROCESSOR DELETES NEW BIOS PROGRAM.
170
CRYPTOGRAPHIC COPROCESSOR ENABLES USE OF NEW BIOS; DELETES OLD BIOS PROGRAM.
180
END.

FIGURE 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/13520

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04K 1/00
US CL : 380/25, 4
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/25, 4

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,421,006 A (JABLON et al.) 30 May 1995.	23
A, P	US 5,584,023 A (HSU) 10 December 1996.	1-23
A	US 5,450,489 A (OSTROVER et al.) 12 September 1995.	1-23

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"B"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
01 DECEMBER 1997	12 JAN 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer DAVID CAIN Telephone No. (703) 305-1836

Form PCT/ISA/210 (second sheet)(July 1992)*